UNIVERSITI PUTRA MALAYSIA

IMPLEMENTATION OF DATA SECURITY SYSTEM IN TABUNG HAJI AND SOCSO

JASMIN ILYANI BT AHMAD

FSKTM 2003 12

IMPLEMENTATION OF DATA SECURITY SYSTEM IN TABUNG HAJI AND SOCSO

JASMIN ILYANI BT AHMAD

MASTER OF SCIENCE

UNIVERSITI PUTRA MALAYSIA

2003

IMPLEMENTATION OF DATA SECURITY SYSTEM IN TABUNG HAJI AND SOCSO

By :

JASMIN ILYANI BT AHMAD

Thesis submitted in partial fulfillment of the requirement for the Master of Science in the Faculty of Computer Science and Information technology

Universiti Putra Malaysia

2003

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirements for the Master Science (Science Computer)

IMPLEMENTATION OF DATA SECURITY SYSTEM IN TABUNG HAJI AND SOCSO

By

JASMIN ILYANI BT AHMAD

October 2003

Supervisor : Pn. Azrina Kamaruddin

Faculty : Faculty of Computer Science and Information Technology

This study is revolves in the data security system that was performed in Social Security Concept (SOCSO) and Tabung Haji. Both organizations used router encryption technique where data that will be transferred will be encrypted and decrypted at router. This situation will cause the original data can be tap or modified by unauthorized users during transfer process, before it sent to the router to be encrypted and after decrypted at the next router. This security was developed to avoid the original data that transferred are being modifies before reach at the router. Besides, this system is developed based on the Caesar cipher technique that was improved its security by adding the key from 25 to 255 keys. With this system, the tap or modified problem can be reduced as well as improving the organizations reliability.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk Master Sains (Sains Komputer)

IMPLEMENTATION OF DATA SECURITY SYSTEM IN TABUNG HAJI AND SOCSO

Oleh

JASMIN ILYANI BT AHMAD

Oktober 2003

Penyelia : Pn. Azrina Kamaruddin

Fakulti : Fakulti Sains Komputer dan Teknologi Maklumat

Kajian ini adalah berkisar kepada sistem keselamatan data yang dijalankan di Social Security Concept (SOCSO) dan Tabung Haji. Organisasi-organisasi ini menggunakan teknik penyulitan router di mana data yang hendak dihantar ke rangkaian akan disulitkan dan dinyahsulitkan pada router. Keadaan ini menyebabkan data asal dapat dicuri atau diubahsuai oleh pengguna tidak sah sewaktu proses penghantaran, sebelum dihantar kepada router untuk disulitkan dan selepas dinyahsulitkan pada router seterusnya. Sistem ini bertujuan untuk mengelakkan data asal yang dihantar dicuri atau diubahsuai sebelum sampai kepada router. Ia dibina berasaskan teknik penyulitan Caesar yang telah diperbaiki tahap keselamatannya dengan menambah bilangan kunci daripada

25 kepada 255 kunci. Sistem ini dapat mengurangkan masalah kecurian atau pengubahsuaian data sekaligus meningkatkan kebolehpercayaan organisasi.

ACKNOWLEDGEMENTS

I would like to express my thanks and gratitude to my supervisor, Pn. Azrina Kmaruddin, for my continual guidance, suggestions, encouragement and moral support in the course of this project. During the project design and development, Pn. Azrina has sacrificed her precious time in providing expertise, advice and general direction. Her contribution is deeply appreciated.

I also wish to thank my course mate, Cik Masrohayatie Talib for providing valuable information, suggestions and encouragement, my ex-course mate, En. Khairul Nizyam Mustaffa for helping out by providing useful feedback throughout the stages of this project, and for all my friends Ida, Moe, Elite, Olie, Iza, Aiman, Awad, Nizam, Shahrul, Kak Ila, Kak Nani, Kak Azi, Kak Mas, Kak Ju, Kak Shita and Kak Lia, who has continuously given a great deal of encouragement and shared opinions and experiences regarding the project. This project would not have been complete without their assistance.

Special thanks go to my parents, En. Ahmad Said and Pn. Nazimah M.Khalid, and the whole family for continually given support, encouragement and for providing suggestion of ideas. Their patience and tolerance have provided motivation and enabled me to persevere throughout this project.

Infinite thanks go to En. Affizal Ahmad for a great deal of encouragement, opinions, ideas, motivation and support regarding this project. His patience is deeply appreciated.

APPROVAL SHEET

The project paper entitled

IMPLEMENTATION OF DATA SECURITY SYSTEM IN TABUNG HAJI AND SOCSO

has been prepared and submitted by

JASMIN ILYANI BT AHMAD

GS 10021

Faculty of Computer Science and Information Technology as partial fulfillment of the requirement for the Degree of

Master of Science (Computer Science)

Approved by

(Pn. Azrina Kamaruddin)

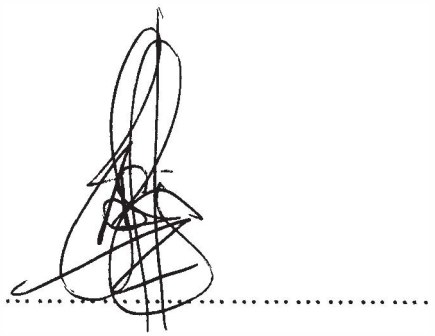
Project Supervisor

October 2003

DECLARATION FORM

DECLARATION

I hereby declare that the work in this dissertation is based on my original work except for quotations and citations, which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Putra Malaysia or other institutions.



JASMIN ILYANI BT AHMAD

Date : 15 October 2003

LIST OF TABLES

TABLES **PAGE**

LIST OF FIGURES

FIGURES **PAGE**

CHAPTER 1

INTRODUCTION

1.0 Introduction

Nowadays the life within cyber technology where data and information are shared together around the world through to Internet and wireless mobile, we still have to face all the fraud related to this latest technologies. Most of transactions today are being done through the Internet technologies so the data transferred are exposed to the hackers.

Some of the hackers just like to hack the data but some of them take the advantages by hacking the system. For instance, in banking transaction, the hackers can change the value of money that are being transferred, and the destination of the transformation. All these kind of problems can effects the banking performance in the world.

In solving and avoiding all those problems, the data that are being transferred will be encrypted to the ciphertext during the transfer process. So, if the hackers hack the encrypted data, it is useless unless they decrypt the data to get the original message. The decryption takes some times and difficult to perform because of the algorithm and formulas that were used in the encryption. So, the data are secured during the transfer process. However, sometimes the hackers can get the original message even we decrypt it

before the transfer process. This is because of the use of simplest encryption algorithm such as the Caesar cipher. Besides, the hackers maybe know the public key or private key that were used in the encryption process. So, the choosing of any kind of encryption algorithm should be based on how secret and confidential the data is and how strong the algorithm that will be used.

1.1Company and Departmental Background

1.1.1 Tabung Haji (TH)

Tabung Haji (TH) as a dynamic corporate Islamic entity that masters the art of managing and handling of pilgrimage matters besides gaining world recognition as a highly efficient body with unquestionable integrity in capitalizing on resources to strengthen Muslims economic equity, Tabung Haji has strong determination and is highly committed to fulfill its pledge including to provide efficient and excellent services.

Tabung Haji (TH) involved in finance, investments and depository activities due to gain the goal. It has the Investment Department that responsible for all matters pertaining to investment and to see all TH's investment activities are done in accordance to Islamic teaching. Finance Department functions as a body that plans, formulates and provides budget for TH based on the individual department's requirements in achieving the organisation's objectives effectively. Besides, the Depository Department is responsible of handling money deposited and withdrawn by depositors at any of the Tabung Haji's offices nationwide regardless whether the transactions are made at Tabung Haji's district, state or headquarters offices and money collected through agents appointed by Tabung

Haji such as Bank Islam, Bank Simpanan Nasional and post offices. So, Tabung Haji is actually used the encryption system in delivering or transfer money in secured environment as they want to increase the effectiveness of their company.

1.1.2 SOCIAL SECURITY CONCEPT (SOCSO)

SOCIAL SECURITY CONCEPT (SOCSO) is committed to ensure socio-economic security of all working Malaysian citizens. SOCSO provides social security for Malaysians. The concept is employees should be protected by social insurance to decrease the sufferings and to provide financial guarantees. Because their activities also involved the financial activities, so they should have secured data transmission over network. This organization also used encryption system in transferring their data in order to increase the reliability and security of their company.

1.2 Problem Statement

1.2.1 Current Situation of Encryption System in SOCSO and Tabung Haji

SOCSO and Tabung Haji as the organizations in this study are using router encryption. Router encryption is when the data only can be encrypted in the router during the transfer process. Besides, the data that were encrypted are pass through Wide Area Network (WAN) and then it will be decrypted in router before it passes to the destination. Below are the Figure 1-1 that shows the data transfer process including the routers that are using in data encryption and decryption process.

In this case, data that will be transfer will pass through Local Area Network (LAN) without any data encryption or compression. Then it will pass through gateway before the

router. It is only will be encrypt in the router where the router is provided with data encryption system. Then the encrypted data or the ciphertext will pass to the Wide Area Network (WAN). During this time the data are secured because it is in the ciphertext style. Then it will be passed to the router to be decrypted to the original message before it reach its destination.

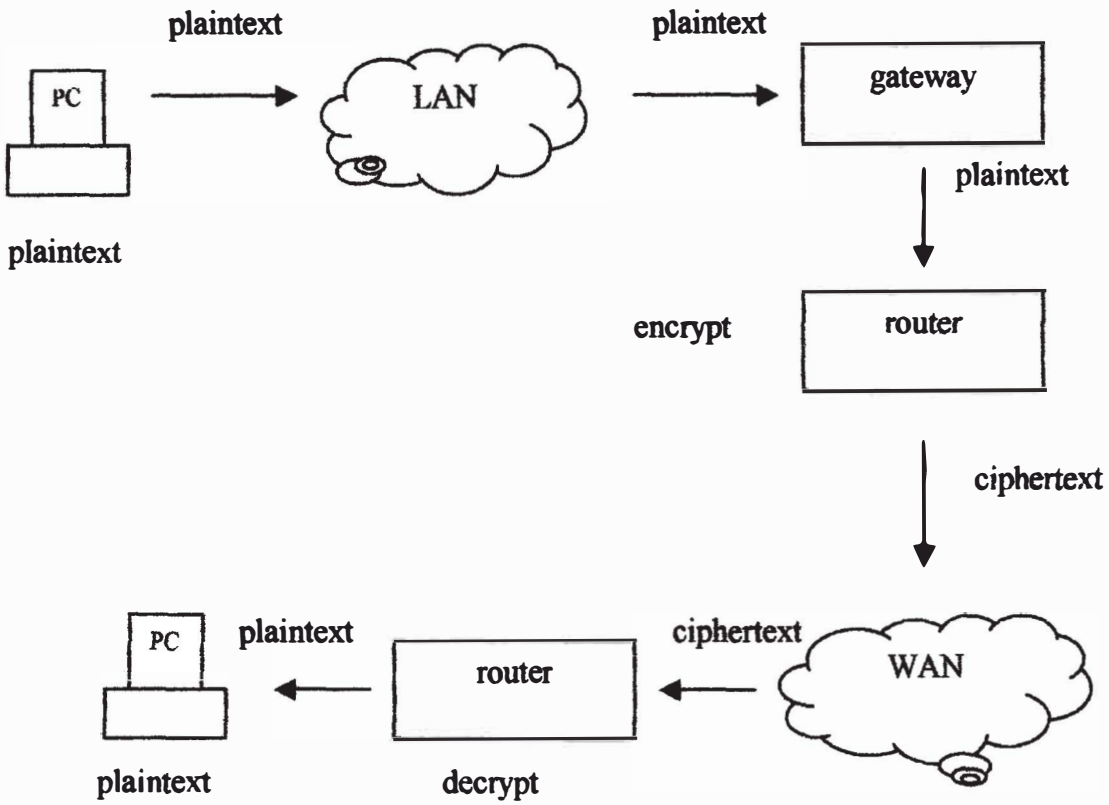


Figure 1-1 : Current situation of SOCSO and Tabung Haji in transferring data through Local Area Network and Wide Area Network.

The problem is data from PC is sent in an original type without any encryption to the Local Area Network. So, data actually is in unsecured environment until it reached at

router and will be encrypted. Then the other problem is after the data reached at the next router and will be decrypted, data is in original pattern that had to be sent to the receiver. This situation can cause the data modified or changed by the unauthorized users or tap by the hackers.

1.2.2 Problems Statements in Current Situation

- Hackers always hack through gateway to access Local Area Network (LAN) to get the original message.
- Besides, the hackers always hack through the active port, which are not in use.
- Sometimes, the configuration of gateway is not configured well.
- The hackers also can hack using the Internet port (Port 80).

1.2.3 Solution of The Problems in Local Area Network (LAN)

To transmit secured data, the encryption system will be used which it starts to encrypt from the sender PC. Then the data will be pass through LAN and WAN as a ciphertext. Then, at the receiver PC, the data will be decrypt to the original message. In this case, not only the router, the PC also will be provided with the data encryption system.

Besides, by performing the encryption system in PC, the risk of hacking the LAN can be reduced. Then, the ciphertext which are the encrypted data will be passed to WAN in a secured environment.

1.3 Objectives

Objective of this study is to avoid data from hackers during the transfer process through the network. This system will ensure that the data are secured from hackers where they can modify, trap and some others Internet crime.

This system will encrypt the original message to the ciphertext using the encryption algorithm. If the hackers can hack the ciphertext during the data transfer, it is useless unless they can decrypt the ciphertext to the original message. However, the hackers should know which algorithm and key that were used in the encryption in order to decrypt the message. So, the data are secured and only the authorize users can get the original message. Besides, this system is developed to decrease the probability 'of hackers in getting the original message in Local Area Network (LAN).

1.4 Scope

The scope of this system is divided into two categories; the users scope and the study scope. This system is an encryption system that can be used by Tabung Haji (TH) and Social Security Concept (SOCSO). This is because the two organizations currently used an existing encryption system without any standard and knowledge of the level of the encryption algorithm they used, whether it is suitable or not to their data.

The users that will be used this system are the system users that involves in data security area. They will use this system to encrypt data during the data transfer process and decrypt the data to the original data when it receives the destination. Besides, this system provides the suitable encryption algorithm to both companies. The system users just can use the system without knowing the standard or level of their data.

This system is performing and operating in Windows environment. It was developed by using Visual Basic but it was performed as an executable file. So, most of company that involves in transferring data or any money transaction through network such as Kumpulan Wang Simpanan Pekerja (KWSP) and Lembaga Hasil Dalam Negeri can adapt this system to be used to encrypt and decrypt data.

1.5 System Requirements

System requirements divided into two categories; hardware requirements and software requirements.

1.5.1 Hardware Requirements

- CPU Intel Pentium 256 MHz
- 128 MB RAM
- 25 MB of memory spaces are needed
- Input devices : keyboard, mouse
- Output devices : printer, monitor